Lutte contre le crime et /ou vie privée

Poullet, Yves

Published in:
Revue Ubiquité. Droit des technologies de l'information

Publication date:
2002

Document Version
le PDF de l'éditeur

Lutte contre le crime et/ou vie privée : un débat difficile !

A propos de l'alinéa 1er du § 2 de l'article 109ter de la loi belge du 21 mars 1991 introduit par la loi belge du 28 novembre 2000 sur la criminalité informatique

*Y. POULLET**

«Si tu es prêt à sacrifier un peu de liberté pour te sentir en sécurité, tu ne mérites ni l'une, ni l'autre»
Benjamin FRANKLIN

1. L'histoire de l'article 109*ter*, E, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques témoigne de la crainte de notre société belge vis-à-vis des atteintes à la sécurité des personnes et des biens, atteintes que permet l'utilisation des technologies nouvelles de l'information et de la communication. Cet article inséré dans la loi récente sur la criminalité informatique impose une collaboration des prestataires de la société de l'information avec les autorités policières et contribue à répondre à cette requête d'un monde sécuritaire. Dans le cadre des suites à donner aux attentats des tours du World Trade Centre, la disposition belge est évoquée dans les débats européens comme un modèle?

Notre propos est d'offrir un commentaire bref de la disposition en même temps que de prendre parti dans le débat «protection des données versus vie privée». A cet égard, nos réflexions puiseront dans les nombreux rapports et avis émis par la Commission à propos de législations récentes en matière de lutte contre la criminalité informatique ou d'interceptions ou écoutes téléphoniques[1].

* Doyen de la Faculté de droit des F.U.N.D.P. de Namur. Directeur du Centre de recherches informatique et droit de Namur

1. A ce propos, outre l'avis de la commission de protection de la vie privée rendu à propos de la loi du 28 novembre 2000 cité ci-après note 3, on rappellera les avis suivants: avis de la commission de la vie privée du 20 mars 1997 sur le projet de loi concernant l'identification et le repérage des numéros de postes de communications ou de télécommunications et portant modification des articles 90*ter*, 90*quater*, 90*sexties* et 90*septies* du Code d'instruction criminelle; avis de la commission de la vie privée du 9 juillet 1997 sur l'application des articles 202 et 203 de la loi du 21 décembre 1994 portant des dispositions sociales et diverses (collaboration technique des opérateurs à l'exécution de mesures judiciaires d'écoute entre autres); avis de la commission de la vie privée du 27 novembre 1997 sur les amendements au projet de loi modifiant la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et télécommunications privées; avis de la commission de la vie privée du 23 mars 1998 sur le projet de loi sur le projet de loi organique des services de renseignement et de sécurité; avis de la commission de la vie privée du 24 mars 1999 sur le projet d'arrêté royal portant exécution des dispositions de la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées et de l'article 109*ter* E, § 2 de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, en ce qui concerne l'obligation pour les opérateurs de réseaux de télécommunication et les fournisseurs de télécommunication de prêter leur concours; avis de la commission de la vie privée du 28 février 2002 sur l'avant-projet de loi «modifiant l'article 44 de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité».

2. La disposition nouvelle astreint sous peine de sanctions pénales les opérateurs de réseaux et les fournisseurs de services de télécommunications à conserver dans les limites du territoire de l'Union européenne, pendant une durée minimale de douze mois, les données d'appel des moyens de télécommunications et d'identification des utilisateurs de services.

On ajoute qu'un arrêté royal délibéré en conseil des ministres après avis de la commission pour la protection de la vie privée déterminera le délai et les données à conserver. Cet arrêté royal n'a point encore été pris.

3. L'examen de cette disposition suit la démarche suivante:

– le premier point conduit à une description analytique de la portée du texte: qu'entend-on par «opérateurs» ou «fournisseurs de services»? Quelles «données» peuvent ou doivent être conservées?
– le deuxième point évoque le débat européen actuel relatif à la lutte contre la cybercriminalité, débat ravivé par les suites des attentats du 11 septembre, en particulier les discussions menées tout au long du parcours qui a conduit à l'adoption de la directive sur la vie privée et le secteur des communications électroniques[2] et les débats relatifs aux dispositions en la matière adoptées par la Convention européenne sur la cybercriminalité[3];
– le troisième point, enfin, critique la disposition légale, objet de l'étude, du point de vue des principes de la protection de la vie privée contenus dans les textes tant internationaux, européens que belges.

1 *La signification de la disposition*

4. La disposition légale[4] complète un texte récemment introduit. La loi du 11 juin 1998 modifiant la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées avait en effet introduit l'obligation de certains prestataires de services de communications de collaborer avec les autorités judiciaires. Selon la loi, le Roi détermine, après avis de la commission de la protection de la vie privée, par arrêté délibéré en conseil des ministres, «les moyens techniques par lesquels les opérateurs de réseaux et les fournisseurs de services doivent permettre le

2. Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, *J.O.C.E.* L.201/37, 31 juillet 2002.
3. Convention européenne sur la cybercriminalité, Conseil de l'Europe, Traité européen n° 185, ouvert à la signature des Etats membres le 23 novembre 2001, Budapest (disponible sur le site du Conseil de l'Europe: http://www.coe.int/treaty/fr/projets/cybercrime.htm).
4. Pour une analyse de cette disposition, le lecteur se réfèrera aux articles publiés sur la loi du 28 novembre 2000 sur la criminalité informatique, ainsi, C. MEUNIER, «La loi du 28 novembre 2000 relative à la criminalité informatique», *in Actualités du droit des technologies de l'information et de la communication*, C.U.P., vol. 45, février 2001, en particulier pp. 151 et s.; Fl. DE VILLENFAGNE et S. DUSOLLIER, «La Belgique sort enfin ses armes contre la cybercriminalité», *A&M*, 2001, pp. 77 et s.; Y. POULLET, «A propos du projet de loi dit n° 214: la lutte contre la cybercriminalité dans le cyberespace à l'épreuve du principe de la régularité des preuves», *in Liber amicorum J. du Jardin* (H. VUYE et Y. POULLET, éd.), Kluwer, 2001, pp. 20 et s. Cf. également, les écrits de P. VAN EECKE, auteur de l'avant-projet de loi en la matière, *Criminaliteit in Cyberspace*, Mijs & Breesch, Gent, 1997, en particulier, pp. 107 et s. et du même auteur, «Het voorontwerp van wet inzake informaticacriminaliteit», *in Recente ontwikkelingen in informatica- en telecommunicatie recht*, I.C.R.I., Die Keure, Brugge, 1999, 238 et s.

repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement de télécommunications privées»[5].

5. La crainte principale[6] exprimée par la commission de protection de la vie privée à l'égard de cette loi était le risque de l'instauration d'une surveillance exploratoire générale: sous réserve des limites que pourrait introduire l'arrêté royal, les autorités judiciaires reçoivent en effet, le droit d'extraire, des banques de données tenues par les opérateurs et fournisseurs de services, des informations permettant une surveillance générale et exploratoire. Cette surveillance générale exploratoire est bannie par les principes établis par la Cour européenne des droits de l'homme sur la base de l'article 8 de la Convention européenne[7].

6. Le complément que la loi du 28 novembre 2000 ajoute à l'alinéa 1er du § 2 amplifie considérablement les moyens donnés à l'autorité policière puisqu'il s'agit de leur permettre d'accéder aux données de communication non seulement en temps réel mais également en temps différé. En effet, est mise à charge des prestataires de services de télécommunications l'obligation, sanctionnée pénalement[8], de mettre à disposition des autorités les données conservées sur le territoire de l'Union européenne[9], et ce pendant au «minimum» 12 mois[10].

5. Un premier projet d'arrêté royal déterminant ces «moyens techniques» avait fait l'objet de vives critiques de la commission (avis n° 12/99 du 24 mars 1999). Un second projet d'arrêté royal est actuellement à l'étude. Cf. à ce propos, l'avis de la commission de protection de la vie privée n° 09/97 du 20 mars 1997 (rapporteurs: B. De Schutter et Y. Poullet) qui notait: «Au regard de telles considérations et dans la mesure où l'article 22 de la Constitution rappelle la nécessité de mesures législatives pour toute dérogation au principe du respect de la vie privée, la commission ne peut admettre que la matière soit réglée par une délégation à un arrêté royal, sans que ne soient fixées les limites strictes de cette intervention royale. La commission rappelle, en particulier, que de telles mesures techniques ne peuvent avoir pour effet de légitimer les pratiques de repérage ou d'interception préventives, qu'elles ne peuvent conduire les autorités publiques à disposer d'informations disproportionnées par rapport à celles nécessaires dans le cadre de l'instruction, enfin qu'elles doivent respecter le caractère strictement d'exception de l'écoute».

6. Avis n° 33/99 du 13 décembre 1999 relatif aux projets de loi relatifs à la criminalité informatique (rapporteurs: B. De Schutter et Y. Poullet), avis disponible sur le site de la commission belge de protection de la vie privée (http://www.privacy.fgov.be) et publié dans les documents parlementaires de la Chambre des représentants (*Doc. parl.*, Chambre, 0213/004). On notera que cet avis a été pris d'initiative par la commission, celle-ci n'ayant pas été consultée par le gouvernement. Cf. également, l'avis très critique du Conseil d'Etat, publié *in Doc. parl.*, 213/002).

7. Nous reviendrons *infra* n° 21 sur les dispositions de la Convention du Conseil de l'Europe sur la cybercriminalité, en particulier l'article 17 qui prévoit une «conservation et divulgation rapides de données relatives au trafic». Cette convention adoptée le 8 novembre 2001 n'existait pas bien entendu lors de l'avis rendu par la commission sur la loi de 1998.

8. Le nouveau § 3 de l'article 109*ter*, E, sanctionne en effet d'un emprisonnement de trois mois à six mois et ou d'une amende de vingt-six francs à vingt mille francs le fournisseur qui n'accomplirait pas ses obligations légales.

9. Le projet mentionnait l'obligation de conservation sur le territoire belge afin d'éviter les questions procédurales de coopération pénale internationale au cas où la demande concernerait des données stockées à l'étranger (cf. les arguments du ministre, *in Doc. parl.*, Chambre, 0213/004, p. 47). La Commission européenne (avis repris *in Doc. parl.*, Chambre, 0213/011, p. 17) s'insurgea contre une disposition jugée contraire aux principes européens de liberté d'établissement et de libre circulation des services. Le gouvernement belge s'inclina devant cette argumentation européenne (*Doc. parl.*, Sénat, 2-392/2, p. 6).

10. Le délai de conservation a été fixé à «au minimum de 12 mois» en dernière minute. La première proposition de loi laissait le soin au Roi de fixer ce délai. La commission avait jugé dans son avis qu'il était nécessaire que le législateur se prononce lui même sur cette durée vu l'impact de cette disposition sur nos libertés individuelles. La commission de protection de la vie privée (avis déjà cité) avait plaidé pour un délai plus court: trois mois comme le préconisent la loi allemande et la recommandation n° 3/99 relative à la conservation des données relatives aux communications pour les offreurs de service Internet en vue d'assurer le respect de la loi du groupe de protection des données institué par l'article 29 de la directive 95/46/C.E., texte disponible sur le site du serveur de l'Union européenne à l'adresse: http://www.europa.eu.int/comm/dg15/fr/media/dataprot/wpdocs. Le débat parlementaire fut acharné entre les partisans d'une conservation longue en réponse aux nécessités des enquêtes policières et ceux qui s'inquiétaient du fait qu'un long délai ne constitue une menace pour les libertés en même temps qu'une charge pour nos entreprises (en ce sens également, l'avis de la Commission européenne repris *in Doc. parl.*, Chambre, 0213/011, p. 18). A l'idée de fixer alors le délai à un maximum de 12 mois, s'est substitué au dernier moment le texte actuel qui fait la part belle aux tenants de la protection de l'ordre public et aux nécessités de l'instruction (sur ce débat, lire *Doc. parl.*, Sénat, 2-392/3, p. 47: l'audition d'un membre de la National Computer Crime Unit et p. 62: la façon dont la balance entre vie privée et ordre public doit s'établir selon le Sénat).

La disposition vise tout «opérateur et fournisseur de services de télécommunications». Par opérateurs de réseaux, on entend tout prestataire offrant des services traditionnels de transport et d'acheminement des messages, qu'il s'agisse de réseaux publics ou privés comme des intranets propres à une administration ou à toute organisation, qu'il s'agisse de réseaux de mobilophonie, hertziens, satellitaires, câbles ou autres.

La notion de «fournisseur de services de communications»[11] élargit encore le champ d'application de la disposition. On songe aux multiples prestataires intervenant dans l'offre de services de l'internet (services d'accès, services de messagerie, *search engines*, portails, services de forum de discussion, etc.) ou dans l'offre de services à valeur ajoutée (services de cryptographie, services de «Trusted Third Parties», services électroniques bancaires,...). On ajoute même les tenanciers de «cybercafés», les serveurs d'«anonymisation», etc.

C'est à l'arrêté royal prévu par la loi[12] de déterminer parmi cette liste, les catégories de services visées par la disposition légale. On notera que la plupart des «opérateurs» ou «fournisseurs» n'ont *a priori* aucune raison de conserver les données au-delà de la durée de connexion[13]. Nombre de ces services sont en effet gratuits. En d'autres termes, la seule finalité de la conservation des données est la manifestation de la vérité dans le contexte de la poursuite d'infractions. Cette constatation a des conséquences sur le fondement de la légitimité des traitements et bien évidemment sur le statut des personnes tenues à cette conservation.

7. Les données à conserver seront fixées également par arrêté royal. Il s'agit, selon le dispositif légal, des données d'appel des moyens de télécommunication[14] et des données d'identification des utilisateurs des services.

La liste de telles données est infinie[15]. Le «Discussion Paper» préparé par les services de la Commission pour la réunion d'experts du 6 novembre relative à la rétention des données relève plus de soixante données susceptibles d'être ainsi collectées et conservées[16]. On notera en effet, à la

11. La notion de «service de communications» se réfère à celle définie par la loi du 21 mars 1991 sur les entreprises publiques autonomes: «service consistant, en tout ou en partie, en la transmission et l'acheminement de signaux par des signaux de télécommunications, à l'exception de la radiodiffusion et de la télévision». Comp. avec la notion de «fournisseur de service» reprise par la Convention du Conseil de l'Europe sur la cybercriminalité (article 1er): «Fournisseur de service» désigne: i) toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique; ii) toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs».
12. La commission belge a critiqué la délégation au Roi en estimant que l'article 22 de la Constitution requérait une loi (avis publié in *Doc. parl.*, Chambre 0213/004, p. 30).
13. A cet égard, la remarque de la commission de protection de la vie privée, *op. cit.*, p. 9.
14. L'exposé des motifs (*Doc. parl.*, Chambre 0213/001, p. 30) précise qu'il s'agira notamment des données relatives à l'origine, la destination, la durée et la localisation des appels. Le Sénat (*Doc. parl.*, 2-392/3, p. 31) estime qu'ainsi les adresses IP des ordinateurs émetteurs et destinataires des télécommunications électroniques, les *logs-in* et les *logs-out*, l'heure et début de la fin de connexion voire les adresses internet visitées font partie des données d'appel.
15. La Commission européenne (avis publié *in Doc. parl.*, Chambre 0213/011, p. 18) a vivement déploré l'absence de toute définition de telles notions. Dans le même sens, les critiques de la commission de protection de la vie privée (avis publié *in Doc. parl.*, Chambre, 0213/004, pp. 30 et s.).
16. L'annexe 2 du Discussion Paper (29 octobre 2001) préparé par les services de la Commission dans le cadre du E.U. Forum on Cybercrime du 27 novembre 2001 et de la réunion d'experts préparatoire du 6 novembre établit la longue liste des types de données susceptibles d'être enregistrées et ce par type de service Internet: ainsi, pour l'e-mail server: SMTP log; date and time of connection of client to server; I.P. adress of sending computer; message ID; sender e-mail adress; receiver e-mail adress; status indicator; POP log or IMAG log; date and time of connection of client connected to server; IP adress; user ID; (in some cases) identifying information of e-mail retrieved; file upload and download servers; pour le FTP (File Transfer Protocol) log, date and time of connection; IP source adress; user ID; path and filename of data object uploaded or downloaded; pour les services Web: http log; date and time of connection; IP source adress; operations (types of command); path of operation; last visited page; response codes;...

suite de J-M. DINANT[17], d'une part, que ces traces se multiplient du fait de l'utilisation de plus en plus généralisée des services de communication dans tous les secteurs de la vie professionnelle et non professionnelle et, d'autre part, que les détenteurs, la nature et le lieu du stockage de ces traces deviennent de moins en moins visibles par l'individu qui les crée et les abandonne au gré des réseaux le plus souvent malgré lui.

Ainsi, lors d'une visite d'un site Web proposé par un serveur quelconque et ce à partir du site d'une société fournisseur d'un service d'indexation automatique (*search engines*) comme Lycos ou Altavista, l'internaute laissera, sans compter les nombreux traitements invisibles possibles, des traces chez le ou les opérateur(s) des réseaux de télécommunications que son message empruntera, chez le fournisseur d'accès et chez les différents serveurs des sites visités. La nature des traces laissées dans l'exemple donné est variée. Si l'opérateur de réseau garde les traces du trafic (le numéro appelant ou plutôt l'adresse du destinataire du message), le fournisseur d'accès peut dans son *logbook* conserver la trace des diverses utilisations opérées à partir du système d'information de l'internaute: les différents sites visités, voire les pages visitées et le parcours suivi, la durée de chaque visite et bien évidemment les caractéristiques de la configuration utilisée par l'internaute. Une même richesse d'information se retrouvera chez l'opérateur du service de recherche et d'indexation automatique voire chez la société de cybermarketing avec laquelle le *search engine* sera connecté par un hyperlien invisible.

8. Les textes européens, ceux de la directive et de la Convention européenne du Conseil de l'Europe, distinguent au sein de ces données, quelques catégories. Ainsi, le Conseil de l'Europe distingue les «données relatives au trafic» et celles «relatives à l'abonné»; l'Union européenne, celles de trafic et celles de localisation. Nous reviendrons sur l'intérêt de telles distinctions[18].

2. *Les débats européens relatifs à l'obligation de conservation des données de trafic*

9. Deux enceintes européennes discutent ou achèvent leurs discussions sur l'obligation de conservation des données de communication et son corollaire: l'obligation de collaboration entre les instances privées, chargées de cette conservation et les instances publiques, autorités judiciaires ou policières.

1. Le Conseil de l'Europe

10. Le Conseil de l'Europe a adopté le 8 novembre 2001 le premier Traité international contre la «cybercriminalité»[19]. Il l'ouvrait à la signature des Etats membres ou non[20], le 23 novembre à l'occasion de la confé-

17. Y. POULLET, J.-M. DINANT, «Le réseau Echelon, existe-t-il? Que peut-il faire? Peut-on et doit-on s'en protéger?», rapport d'expertise rédigé à l'attention du comité permanent de contrôle des services de renseignements, mai 2000, doc. confidentiel, p. 6; cf. du même auteur, l'excellent rapport rédigé pour le projet européen ECLIP, disponible à http://www.droit.fundp.ac.be/textes/privacy_law_tech_convergence.rtf.
18. *Infra*, nº 20.
19. Sur cette convention, parmi d'autres commentaires, relevons: E.M. GNING, «Le projet de convention sur la criminalité dans le cyberespace», *Lex Electronica*, vol. 6, nº 2, 2001 disponible à http://www.lex-electronica.org/articles/v6-2/gning.htm; L. COSTES, «La Convention du Conseil de l'Europe du 8 novembre 2001: premier traité international contre la "cybercriminalité"», *Lamy - Cahiers droit de l'informatique*, nº 142, décembre 2001, 1 à 9.
20. Ainsi, les Etats-Unis, non-membres du Conseil de l'Europe, ont signé la Convention le jour même de l'ouverture de celle-ci à la signature des Etats.

rence de Budapest.

Le texte fait suite à la recommandation nº R(95)13 du comité des ministres relative aux problèmes de procédure pénale liés à la technologie de l'information[21]. Il est le fruit des travaux d'un comité créé dès 1997 chargé d'élaborer une convention sur la cybercriminalité dans le cyberespace et de renforcer ainsi la coopération internationale.

La recommandation se limitait à prescrire des «obligations spécifiques... pour les fournisseurs de services qui offrent des services de télécommunications au public via des réseaux de communication publics ou privés, de délivrer l'information nécessaire, lorsque les autorités compétentes chargées de l'enquête l'ordonnent, pour identifier l'utilisateur». Il s'agissait donc essentiellement dans le cas d'une enquête de permettre aux autorités policières de réclamer l'identité d'un abonné ou d'un client et ce, à partir d'une adresse TCP/IP ou d'un numéro téléphonique ou de mobilophone. La Convention de 2001 contient diverses obligations pour les Etats signataires, étant entendu, rappelle l'article 15, que la mise en oeuvre des règles prévues doit être soumise «aux conditions et sauvegardes prévues par son droit interne qui doit assurer une protection adéquate des droits de l'homme et des libertés». Ce principe général induit clairement le devoir d'un respect de l'article 8 de la Convention européenne des droits de l'homme et de la jurisprudence qui l'a suivi et interprété.

11. La première obligation concerne la conservation «rapide» (expéditions) de données spécifiques y compris des données de trafic qui ont été stockées au moyen d'un système informatique. Elle incombe aux personnes gardiennes de ces données («in the person's possession or control») et l'article 16 prévoit que cette conservation rapide a une durée maximale de nonante jours[22] éventuellement renouvelable. Cette disposition est loin d'avoir la portée générale de la disposition belge. Elle vise dans le cadre d'une enquête relative à une infraction déterminée, le droit des autorités de demander à une personne déjà en possession de certaines données de les conserver pour éviter leur disparition. Elle n'autorise pas l'Etat à réclamer des opérateurs ou fournisseurs des devoirs supplémentaires de collecte de données et surtout pas à opérer cette conservation vis-à-vis de toutes les utilisations de son ou ses services[23].

12. L'article 17 souligne que la conservation et la divulgation des données conservées sur la base de l'article 16 se conçoit d'un nombre suffisant de données de trafic de manière à permettre «l'identification des fournisseurs de services et de la voie par laquelle la communication a été transmise».

A côté de ce premier prescrit, l'article 18 de la Convention crée l'obligation pour les Etats membres d'introduire des dispositions permettant aux autorités compétentes d'ordonner «à un fournisseur de service de «communiquer les données relatives à l'abonné qui sont en possession ou sous le contrôle de ce fournisseur de services». L'article 18 prévoit que par «données relatives aux abonnés», il faut entendre exclusivement les données portant « sur l'identification des personnes utilisatrices des services fournis par les opérateurs et

21. Disponible à http://www.coe.fr/cm/ta/rec/1995/f95r13.htm.
22. La durée de conservation d'un an avait été prévue. Elle a été sévèrement réduite suite à la pression des autorités de contrôle en matière de protection des données et des associations de défense des libertés.
23. Il est à noter que le Parlement européen dans son avis du 6 septembre 2001 avait insisté sur le fait qu'«il ne doit pas être établi de principe général de conservation».

sur les caractéristiques techniques des services fournis par les opérateurs et sur les caractéristiques techniques des communications assurées par ces derniers. Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultables sous quelque forme que ce soit, dans le cadre de ces communications».

On notera que le devoir de production ainsi prévu ne concerne que des données déjà traitées par le fournisseur de service dans le cadre normal de ses activités et ne vise que les données dites de connexion, c'est-à-dire les données relatives à l'identité des personnes qui se connectent au service à l'exclusion des données dites de trafic, ainsi la liste des sites visités, la durée de connexion, etc.

Cette exclusion des données quant à l'utilisation du service est le fruit de longs débats et en particulier des oppositions marquées d'une série d'associations américaines et européennes de défense des libertés[24] de même que du groupe européen de protection des personnes à l'égard du traitement des données à caractère personnel dit groupe de l'article 29[25].

2. L'Union européenne

13. La position européenne qui a toujours privilégié l'approche «protection des libertés» s'est trouvée singulièrement mise en cause à la suite des attentats du 11 septembre sur le sol américain.

Illustre particulièrement bien la première approche européenne, la réaction de nombreuses instances européennes à la découverte du réseau d'écoutes appelé Echelon[26]. Ce réseau géré principalement par les Etats-Unis, permettait aux services d'intercepter et d'analyser les messages ou certains messages transitant par satellites, qu'il s'agisse de communications téléphoniques ou électroniques. Certes, les réactions furent lentes à venir depuis le rapport S.T.O.A. de 1998[27] et ce en raison de la participation du Royaume-Uni au réseau Echelon, de la présence de bases d'écoutes en Allemagne et en Angleterre et finalement de l'existence d'un réseau français concurrent. Elles devaient cependant aboutir, grâce notamment à l'intervention du groupe européen de protection des données[28], à une résolution votée par le Parlement européen le 5 septembre 2001 dans la foulée du rapport Schmidt. On y lit notamment parmi les considérants, une condamnation des pratiques d'interception non conformes aux principes de la Convention européenne des droits de l'homme.

14. La volonté européenne de protéger la vie privée des citoyens européens dans le cyberespace se fonde, à l'intérieur de l'Europe, sur la reconnaissance

24. Ainsi, on soulignera le rôle joué par l'EPIC (U.S.), le Privacy International (UK) et l'Electronic Frontier Foundation.
25. A cet égard, de manière très nette, la recommandation 2/99 concernant le respect de la vie privée dans le contexte de l'interception des télécommunications adoptée le 3 mai 1999 (WP 18, 5005 99/final).
26. Sur ce réseau, lire le rapport d'expertise rédigé à l'attention du comité belge de surveillance des services de renseignements par Yves POULLET et J-M. DINANT, «Le réseau Echelon - Existe-t-il? Que peut-il faire? Peut-on et doit-on s'en protéger?», disponible à http://www.crid.ac.be/ et surtout la remarquable étude de D. YERNAULT, «De la fiction à la réalité: le programme d'espionnage électronique global "Echelon" et la responsabilité internationale des Etats au regard de la Convention européenne des droits de l'homme», *Rev. belge de droit int.*, 2000, pp. 136 et s.
27. Cf. le rapport «Une évaluation des techniques de contrôle politique (sept. 98) et plusieurs études (avril et mai 1999) publiés par le S.T.O.A. (Scientific and Technological Options Assessment) du Parlement européen.
28. Cf. en particulier, la recommandation concernant le respect de la vie privée dans le contexte de l'interception des télécommunications (recommandation 2/99 du 3 mai 1999, doc. 5005/99 final WP. 18 disponible à l'adresse http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs.

de la protection des données comme droit fondamental[29], qu'à l'extérieur, sur une vision moderne du principe de souveraineté[30]. Elle doit cependant tenir compte d'impératifs de sécurité et en particulier de la lutte contre la cybercriminalité. Depuis le Traité d'Amsterdam, l'Europe est compétente à prendre des initiatives fondées sur le troisième pilier[31], à savoir la coopération intergouvernementale dans les domaines de la justice tant civile *que pénale* et des affaires intérieures. Cette nécessité d'un équilibre est affirmée par une communication de la Commission en date du 26 janvier 2001[32]: «La présente communication s'interroge sur la nécessité d'une initiative en vue de définir une politique globale et étudie les différentes formes qu'elle pourrait prendre, dans le contexte des objectifs plus larges que constituent la société de l'information et la création d'un espace de liberté, de sécurité et de justice, en vue d'améliorer la sécurité des infrastructures de l'information et de lutter contre la criminalité informatique, dans le respect des droits fondamentaux de la personne, conformément à l'engagement pris par l'Union européenne».

Appliquant le principe d'une balance à l'obligation de stockage de certaines données de trafic, la communication distinguait celles traitées par les opérateurs et fournisseurs de services dans le cadre normal de leurs activités de facturation[33] et celles qui obligeraient les opérateurs et les fournisseurs de service à traiter des données aux seules fins d'enquêtes pénales. A l'égard des premiers, la Commission estime que les Etats membres peuvent adopter des mesures législatives visant à limiter la portée de cette obligation d'effacement des données relatives au trafic lorsqu'une telle limitation constitue une mesure nécessaire, entre autres, pour la prévention, la recherche, la détection et la poursuite d'infractions pénales ou pour l'utilisation non autorisée du système de télécommunications[34].

29. A cet égard, on relève que le traité de Nice qui fixe la Charte européenne des droits fondamentaux, distingue clairement la protection de la vie privée et familiale (conception traditionnelle de la *privacy*), visée par l'article 6 et la protection des données (conception moderne et élargie de la *privacy*). Sur cette distinction, nos remarques *in* «Pour une justification des articles 25, 26 et 4 de la directive 95/46 en matière de protection des données», *paper* présenté à la Conférence internationale organisée par la Commission européenne sur la transposition de la directive 95/46/CE (30 sept. - 1 oct. 2002), à paraître.
30. Sur l'évolution de ce concept dans la société globale de l'information, nos remarques *in* Y. POULLET et J.-M. DINANT, «Le réseau Echelon», article cité.
31. Sur les particularités de ce troisième pilier, ses procédures particulières et ses mérites, lire D. VIGNES, «Plaidoyer pour le troisième pilier», *Rev. marché commun*, 1996, pp. 273 et s. En matière de criminalité informatique, la Commission a récemment introduit dans le cadre de ce troisième pilier une proposition de décision-cadre du Conseil relative aux attaques visant les systèmes d'information (Bruxelles, le 19 avril 2002, COM(2002)173 final). Cette proposition cherche à harmoniser la définition des infractions en la matière et à définir la compétence de chaque Etat membre quant à la poursuite de telles infractions ainsi que leur collaboration.
32. Communication de la Commission au Conseil, au Parlement européen, au comité économique et social et au comité des régions: «Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité», Bruxelles, COM(2000)890 final.
33. Conformément aux directives communautaires sur la protection des données à caractère personnel, et plus précisément au principe général de limitation des transferts à une finalité spécifique énoncé dans la directive 95/46/CE et aux dispositions particulières contenues dans la directive 97/66/CE, les données relatives au trafic doivent être effacées ou rendues anonymes dès que le service de télécommunications a été fourni, sauf lorsqu'elles sont nécessaires à des fins de facturation. Dans le cas d'un accès forfaitaire ou gratuit aux services de télécommunications, les fournisseurs de services ne sont pas autorisés, en principe, à conserver les données relatives au trafic.
34. La communication précise, se faisant d'ailleurs l'écho des dispositions de l'article 14 de la directive 97/66/CE et de l'article 13 de la directive 95/16.CE que: «Cependant toute mesure législative prise à l'échelon national qui prévoirait la conservation des données relatives au trafic pour les besoins de l'application des lois devrait remplir certaines conditions. Les mesures proposées devraient en effet être appropriées, nécessaires et proportionnées au but poursuivi, comme le prévoient le droit communautaire et le droit international, notamment la directive 97/66/CE et la directive 95/46/CE, la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 et la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Le respect de ces conditions et de ces principes serait d'autant plus important pour les mesures qui impliquent la conservation systématique des données sur une large fraction de la population.

Vis-à-vis du second type de données, la Commission énonce que leur enregistrement et leur conservation ne peuvent se justifier que pour des raisons exceptionnelles et pour une durée très limitée.

A cet égard, elle évoque la résolution du Parlement européen qui, dans une matière très particulière, la lutte contre la pornographie enfantine, a admis à titre tout à fait exceptionnel la conservation des données relatives au trafic pendant une durée de trois mois[35].

15. Les attentats du 11 septembre ont justifié la demande insistante de l'administration américaine d'une meilleure collaboration des Etats européens à la lutte contre le terrorisme et en particulier de revoir les mécanismes de protection des données informatiques de manière à assurer une lutte efficace contre les réseaux terroristes opérant notamment via les réseaux modernes de communication[36]. On notera que dans un temps record, «with all the urgency of a nation at war», la Maison-Blanche avait fait adopter par le Congrès un certain nombre de textes législatifs pour permettre une lutte efficace contre le terrorisme, en particulier le Patriot Act[37] dont certaines dispositions concernent les écoutes téléphoniques[38]. A propos de ces dispositions, on notera que les dispositions américaines ne prévoient pas d'obligation de stockage des données de trafic pour les prestataires de service de communications au-delà de ceux nécessités par les services offerts par ces derniers[39]; que la communication de telles données conservées n'est pas imposée mais se fait sur une base volontaire dans le cadre de «codes of conduct» élaborés entre ces prestataires et les autorités judiciaires ou de sécurité; enfin que les obligations de communiquer les données de trafic sont entourées de nombre de garanties procédurales et de sanctions pénales et civiles en cas de non-respect des conditions légales imposées par le texte légal[40] et ne peuvent en aucune manière donner lieu à un accès au contenu des communications[41]. Enfin, sous la pression des lobbies des défenseurs des libertés, la loi prévoit une clause de «Sunset»[42], qui limite à quatre ans la durée de vie des dispositions légales.

35. Résolution législative portant avis du Parlement européen sur le projet d'action commune - adopté par le Conseil sur la base de l'article K.3 du Traité sur l'Union européenne - relative à la lutte contre la pornographie enfantine sur Internet, amendement 17 (*J.O.* - 219, 30 juillet 1999, p. 68).
36. Cf. notamment les articles publiés par les journaux en octobre à la suite des discussions entre le président G. Bush et le premier ministre belge, la Belgique assumant alors la présidence de l'Union européenne, ainsi, notamment, la *Libre Belgique* du 22 octobre 2001; *Gazet van Antwerpen* du 26 octobre 2001.
37. «Uniting and Strenghtening America by providing Appropriate Tools Required to Intercept and Obstruct Terrorism» (USA Patriot Act), Act of 2001, H.R. 3162, 1st session, 107 th Congress, disponible sur le site http://thomas.loc.gov, approuvé par le Sénat le 25 octobre et signé par le président Bush le 26 octobre.
38. A cet égard, on notera les déclarations de Bush à la suite de l'adoption de cette loi, lors de la signature présidentielle de la loi: «This law will give intelligence and law enforcement officials new tools to fight a present danger... to counter a threat like no other our nation has ever faced».
39. Sect. 222: «Nothing in this Act shall impose any additional technical obligation or requirement on a provider of a wire or electronic communication service or other person to furnish facilities or technical assistance...».
40. Sect. 223: «Civil Liability for certain unauthorized disclosure».
41. Sect. 212 insérant notamment un ' 2703 «Required disclosure of customer communications or records»: «A provider of electronic communications service or remote computing service shall disclose a record or other information pertaining to a subscriber or to a customer of such service (not including the contents of communications covered...) to a governmental entity».
42. Sect. 224. A propos de ces mesures qui assurent selon le sénateur T. Dashle, «an appropriate balance between protecting civil liberties, privacy and ensuring that law enforcement has the tools to do what it must»: «Negotiators have placed safeguards on the legislation, like a four-year expiration date on the wiretapping and electronic surveillance portion, court permission before snooping into suspects' formerly private educational records and court oversights over the FBI's use of a powerful e-mail wiretap system» (J.-J. HOLLAND, «Senate sends Antiterrorism Legislation to Bush», texte disponible à: http://www.washingtonpost.com /wp-dyn/articles/A51682-2001Oct25.html).

16. La discussion entamée dès 2000 de la révision de la directive 97/66 concernant le traitement des données à caractère personnel et la protection des données dans le secteur des télécommunications[43] devait fournir le cadre principal de cette réponse européenne à la demande américaine. Cette proposition de directive était à l'origine intégrée dans un ensemble de propositions visant à réformer la réglementation des télécommunications européennes[44] afin de l'adapter aux développements technologiques et du marché des services des télécommunications. La proposition devenue projet a été l'objet d'une «Position commune arrêtée par le Conseil en vue de l'adoption de la directive» [45]. La directive concernant les traitements de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques a finalement été adoptée le 12 juillet 2002[46].

La proposition initiale énonçait le principe suivant lequel les données de trafic et de localisation ne pouvaient être conservées et utilisées, sauf consentement exprès du client dans le cadre de l'offre de services à valeur ajoutée, qu'aux fins de facturation et d'interconnexion. Cette proposition initiale reprenait la solution déjà affirmée par la directive 97/66. Lors des discussions qui ont précédé les événements dramatiques du 11 septembre, le conseil des ministres du 27 juin des télécommunications avait déjà été sensible[47] aux demandes venant de certaines autorités policières en acceptant l'ajout d'une phrase au considérant n°10 du préambule[48]: «cette directive n'affecte pas le droit des Etats membres de mener des interceptions légitimes de communications électroniques ou de prendre d'autres mesures telle que d'ordonner la conservation des données de trafic ou de localisation pour une période limitée quand cette conservation est nécessaire et justifiée pour ces raisons et en conformité avec les principes généraux du droit communautaire.

Les suites des attentats provoquèrent des discussions importantes en la matière. Le 20 septembre, la réunion des ministres européens de la Justice et des Affaires intérieures adopte des conclusions qui requièrent que tous les fournisseurs de télécommunications conservent les données et y donnent accès aux autorités policières «à des fins d'enquêtes criminelles» et réclame de la Commission européenne la révision de la législation européenne de manière à garantir une contribution aux efforts des autorités en charge de l'application des lois pénales[49].

17. Pour répondre à cette demande relayée aussitôt par les autorités policières, la Commission organisa le 27 novembre 2001 un *hearing* à Bru-

43. *J.O.*, L.24, 30 janv. 1998, p. 1.
44. Sur cette position commune, lire Y. POULLET, S. LOUVEAUX et M.V. PEREZ-ASINARI, «Data Protection and privacy» *in Global Networks: An European Approach, E.D.I. Law Review*, 2001, 147 et s.
45. La position commune a été adoptée par le Conseil, le 21 janvier 2002 (Dossier institutionnel 2000/0189, COD, 15396/01).
46. Directive 2002/58/CE, *J.O.*, L.201/37, 31 juill. 2002.
47. Sous la pression des gouvernements français et anglais.
48. La Commission par la voix de son commissaire E. Likkanen avait insisté sur le fait qu'une telle clause ne pouvait avoir que le statut d'un «recital» et ne devait pas être incluse dans le texte de la Convention.
49. «The Council requests that European commission to submit proposals for ensuring that law enforcement authorities are able to investigate criminal acts involving the use of electronic communications systems and to take legal measures against their perpatrators. In this context, the Council will be making a particular effort to strike a balance between the protection of personal data and the law enforcement authorities' need to gain access to data for the purposes of criminal investigations» (sur ces conclusions, lire le rapport de l'association anglaise Statewatch, «EU governments want the retention of all telmecommunications data for general use by law enforcement agencies under terrorism plan», disponible à http:// www.statewatch.org /news/2001/sep/20authoritarian.htm.).

xelles sur le cybercrime[50]. Cette réunion fut précédée d'une réunion d'experts le 6 novembre ayant pour objet unique la conservation des données de trafic[51] rassemblant des représentants des autorités de protection des données, des autorités policières et de l'industrie. Il ressort de ces discussions menées à la fois lors de la réunion d'experts et lors de l'audition du 27 novembre:

– du côté de l'industrie, un double point de vue: celui des fournisseurs de services de télécommunication[52] de pouvoir opérer une conservation des données à des fins de sécurité de leurs propres systèmes d'information et des mêmes personnes leur malaise de devoir collaborer «gratuitement» à des demandes d'autorités bien souvent mal libellées ou vagues; celui des ayants droit des titulaires de droit d'auteur d'utiliser les compétences policières qui pourraient être reconnues pour mieux lutter contre la cybercriminalité que constitue le copiage illicite d'oeuvres sur le réseau;
– celui des autorités de protection des données[53] de s'opposer à la conservation des données au-delà des strictes nécessités de la facturation et de manière plus générale de définir des mesures procédurales de telle manière qu'elles soient en parfaite conformité avec les droits fondamentaux et les libertés des citoyens et avec les législations de protection des données: ainsi, les commissaires à la protection des données rappellent l'interdiction de toute mesure générale de surveillance et la nécessité de justification concrète pour la rétention de données de trafic spécifiées. Enfin, «la durée de rétention des données et le nombre de données doivent être en proportion avec la gravité de l'infraction criminelle». Enfin, les autorités de protection des données soulignent le caractère très sensible des données de trafic qui révèlent le comportement d'un individu dans la mesure de la généralisation croissante de l'utilisation des moyens de télécommunications dans la vie courante;
– celui des autorités policières qui considèrent comme vitale la possibilité pour la police de résoudre des cas grâce à la conservation des données de trafic et de localisation et à la collaboration convenue ou imposée par la loi des fournisseurs

50. Un premier *hearing* avait été organisé le 7 mars 2001 à propos de sa communication sur le cybercrime de manière à permettre aux représentants de chaque catégorie d'intérêts (opérateurs de réseaux; fournisseurs de service; autorités policières; autorités de protection des données; association de libertés) de faire valoir leur point de vue.
51. A propos de cette réunion, cf. le discussion paper préparé par les services de la Commission et disponible sur le site de la Commission à l'adresse: http://europa.eu.int/information_society/topics/telecoms/internet/crime/wpapnov/index.htm.
52. Cf. en particulier la position d'AOL: «AOL retains only data that is necessary either for billing purposes, fraud prevention or security». «AOL cannot cost a potential data retention obligation without understanding fully what would be required from us. However, some costs consideration would be, not only the storing of data but more importantly the cost of keeping the integrity of the data and the costs associated with data retrieval». Cf. également la position de l'European Association of Consumers Electronic Manufacturers (E.I.C.T.A.) et de l'E.A.C.E.M. qui estiment que l'obligation de conservation de données impose des charges financières importantes aux fournisseurs de service et s'opposent à toute conservation obligatoire des données de trafic sauf dans le cas de poursuites relatives à des infractions déterminées: «Under a data preservation order, service providers store data related to a particular person, rather than store all users' data for potential future investigations. Because data preservation requirements are directed at particular person or persons, they do not pose the same privacy concerns as general data retention».
53. A ce propos, l'intervention de P.Schaar à la réunion d'experts du 6 novembre 2001 et celle de D. Smith au *hearing* du 27 novembre. On se référera en outre aux «opinions» émises par le groupe de protection des données de l'article 29, en particulier, la dernière (5074 final) adoptée le 5 novembre 2001 à propos de la Communication de la Commission: «Creating a safer information Society by improving the security of information infrastructures and combating computer-related crime» (disponible à http://europa.eu.int/commm/internal_market/en/dataprot/wpdocs/index.htm;) et aux travaux de l'International Working Group on Data Protection in Telecommunications, «Common Position on Data Protection aspects in the Draft Convention of Cybercrime of the Council of Europe», 13-14 sept. 2000, texte disponible à l'adresse: http://www.datenschutz-berlin.de/doc/int/iwgdpt/cv_en.htm.

de services de télécommunications. Ces autorités soulignent que cette nécessité est absolue pour certains types d'infraction[54] dans la mesure où sans cette conservation et collaboration, il leur serait impossible de détecter les criminels. Enfin, les autorités policières justifient la longue liste des données de trafic à conserver et les durées de conservation (entre 6 mois et deux ans).

18. Les autorités européennes devaient tirer les conclusions de ces débats en modifiant légèrement le texte de la proposition de directive. Ainsi, le texte final élargit les finalités légitimes pour lesquelles les fournisseurs de réseaux ou de services de télécommunications peuvent traiter les données de trafic ou de localisation. L'article 6.5 ajoute au texte initial la finalité de détection des fraudes et le traitement en vue de la commercialisation de services à valeur ajoutée n'est plus soumis au consentement de la personne concernée, ces traitements devant se limiter, précise le texte, à ce qui est nécessaire à de telles activités. Surtout, l'article 15 autorise les Etats membres à «adopter des mesures législatives visant à limiter les droits et obligations prévus aux articles 5 et 6, à l'article 8, §§ 1er, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'Etat – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, § 1er, de la directive 95/46/C.E.». A cette fin, ajoute le texte, «les Etats membres peuvent, entre autres, prévoir la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe, dans le respect des principes généraux du droit communautaire»[55].

19. Le texte ainsi revu laisse chaque Etat libre de procéder comme il le souhaite mais impose le respect de ce qui, selon l'article 6 du Traité du 7 février 1992 sur l'Union européenne[56], constitue un principe général de l'Union européenne: le respect des droits de l'homme et des libertés fondamentales «tels qu'ils sont garantis par la Convention européenne des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 et tels qu'ils résultent des traditions constitutionnelles communes aux Etats membres». En d'autres termes, le texte renvoie à l'obligation des Etats

54. Cf. en particulier, l'audition de l'autorité policière norvégienne qui relève en particulier les infractions suivantes: «breaking into computer systems; theft of trade secrets; sabotage of critical IT systems; abuse of telephone systems; fraud;threats of life and health; blackmail; harassement and defamation...».

55. Le considérant nº 11 note: «A l'instar de la directive 95/46/CE, la présente directive ne traite pas des questions de protection des droits et libertés fondamentaux liées à des activités qui ne sont pas régies par le droit communautaire. Elle ne modifie donc pas l'équilibre existant entre le droit des personnes à une vie privée et la possibilité dont disposent les États membres de prendre des mesures telles que celles visées à l'article 15, § 1er, de la présente directive, nécessaires pour la protection de la sécurité publique, de la défense, de la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) et de l'application du droit pénal. Par conséquent, la présente directive ne porte pas atteinte à la faculté des Etats membres de procéder aux interceptions légales des communications électroniques ou d'arrêter d'autres mesures si cela s'avère nécessaire pour atteindre l'un quelconque des buts précités, dans le respect de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, telle qu'interprétée par la Cour européenne des droits de l'homme dans ses arrêts. Lesdites mesures doivent être appropriées, rigoureusement proportionnées au but poursuivi et nécessaires dans une société démocratique. Elles devraient également être subordonnées à des garanties appropriées, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales».

56. *J.O.C.E.*, C.191, 29 juillet 1992 et *M.B.*, 30 octobre 1993.

membres de respecter l'article 8 de la Convention et, selon les auteurs[57], la jurisprudence de la Cour strasbourgeoise prise en application de cet article 8 comme source d'inspiration privilégiée du droit communautaire.

Ce devoir de respect de la Convention n'interdit cependant pas des divergences d'interprétation entre les Etats membres quant à la portée précise à donner à cette référence. En ce sens, il ne répond pas aux objections des fournisseurs de services, inquiets des différences d'interprétation que pourrait donner chaque Etat membre à une disposition aussi floue quant à la durée de conservation, quant aux données à conserver et quant aux modalités de cette conservation; elle heurte les principes de protection des données tels que les autorités de protection des données les avaient interprétés; enfin, tout en leur donnant raison sur le principe de la conservation des données, elle renvoie les juges et policiers à leurs gouvernements nationaux pour obtenir une légalisation nationale de l'obligation de conservation et de collaboration des fournisseurs d'infrastructure et de services. On note que dès le 31 octobre, le législateur français devait, dans le cadre de la loi sur la sécurité quotidienne[58], utiliser cette compétence laissée aux législateurs nationaux en des textes sur la teneur desquelles nous reviendrons dans l'analyse critique, objet du point III. Notons cependant que le texte de la directive européenne confie au groupe dit de l'article 29, composé de représentants des diverses autorités de protection des données un rôle important dans l'interprétation à donner au texte communautaire, ce qui peut prévenir des divergences nationales ou des interprétations trop laxistes du texte[59].

Analyse critique
Pistes pour le suivi de l'obligation légale de conservation des données et de collaboration des fournisseurs de services de télécommunications

20. Les compléments du paragraphe 2 de l'article 109*ter*, E, apportés par la loi sur la criminalité informatique apparaissent donc comme une transcription anticipée d'une directive en voie d'approbation. Notre souci est dans ce dernier point de proposer quelques réflexions qui puissent servir de guide à la réglementation qui donnera à la loi sa pleine efficacité en

57. J. RIDEAU et J.-F. RENUCCI, «Dualité de la protection juridictionnelle des droits fondamentaux: atout ou faiblesses de la sauvegarde des droits de l'homme?», *Justices*, 1997, nº 6, pp. 95 et s.; F. PICOD, «Le juge communautaire et l'interprétation européenne» *in* F. SUDRE (éd.), *L'interprétation de la Convention européenne*, Bruylant, 1998, pp. 289 et s. qui parle de «phase de connaissance et d'exploitation» de la jurisprudence de Strasbourg par la CJCE. A cet égard, la liste impressionnante d'arrêts de la Cour de justice des Communautés européennes, reprise par RENUCCI, *in Droit européen des droits de l'homme, L.G.D.J.*, 2e éd., 2001, p. 339.

58. Loi nº 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, *J.O.*, 16 nov. 2001.

59. L'article 15.3. stipule expressément que: «Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, institué par l'article 29 de la directive 95/46/CE, remplit aussi les tâches visées à l'article 30 de ladite directive en ce qui concerne les matières couvertes par la présente directive, à savoir la protection des droits et des libertés fondamentaux ainsi que des intérêts légitimes dans le secteur des communications électroniques». Cet élargissement explicite des compétences du groupe 29 est remarquable. Elle permet notamment à ce dernier organe conformément à l'article 30.2 et 3 de la directive 95/46 d'émettre des recommandations sur l'interprétation à donner au texte et surtout, s'il constate des divergences susceptibles de porter atteinte à l'équivalence des protections du fait des législations ou de pratiques d'Etats membres d'informer la Commission qui pourra alors selon le mécanisme prévu par le texte de la directive 2002/58/CE instruire une modification du texte de la directive.

même temps que nous reviendrons sur les choix opérés par nos législateurs.

Notre première réflexion est liminaire. Elle souligne l'importance des données dont il est question lorsqu'on parle des données de localisation ou de trafic. La notion de données de trafic est définie par le législateur européen comme «toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation» et celle de «données de localisation» comme «toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public». De telles données sont infinies: elles comprennent outre les données de simple connexion, leur durée, les destinataires de nos messages, les sites visités, la longueur des messages échangés, les caractéristiques du message et du système d'information de l'utilisateur; les données de localisation révèlent à quelques mètres près l'endroit où se trouvent un mobilophone ou un G.P.S. même non en cours d'utilisation. C'est que l'utilisation de plus en plus intensive des technologies de l'information et la multiplication de services à valeur ajoutée qui leur sont attachés trahissent les relations que nous nouons avec autrui, de nos déplacements, de nos goûts, nos convictions voire nos maladies, elles laissent en effet chez des intervenants de plus en plus nombreux et divers, des traces de plus en plus nombreuses en des lieux certes disparates mais certes susceptibles d'être reliés grâce aux vertus des réseaux et de systèmes de plus en plus performants de traitement de l'information.

Bref, la possibilité d'avoir accès à ces multiples fichiers et de pouvoir croiser les données y contenues crée des possibilités bien tentantes pour l'autorité policière ou judiciaire. Au-delà, on s'interroge sur la possibilité de maintenir une distinction entre les données de trafic et de contenu. Cette distinction parfaitement claire lorsqu'il s'agissait des données relatives aux communications téléphoniques traditionnelles où les données relatives aux correspondants d'une communication et à leur localisation dans le temps et la durée, s'efface en effet lorsque dans les réseaux modernes, la donnée dite de trafic révèle le contenu même de la communication, ainsi l'accès à une page Web voire à un site Web révèle le contenu de la communication.

21. Faut-il introduire dès lors des limites à ce stockage, des modalités particulières à cette opération et aux possibilités d'accès des autorités chargées de la poursuite des infractions? On rappellera à cet égard, l'arrêt fondamental de la Cour européenne des droits de l'homme, dit arrêt *Klass* du 6 septembre 1978, où la Cour reconnaît le pouvoir discrétionnaire des Etats quant au choix des systèmes de surveillance auxquels ils peuvent avoir recours mais souligne que ce pouvoir discrétionnaire ne signifie pas un pouvoir arbitraire: «Consciente du danger inhérent à pareille loi de saper voire de détruire la démocratie au motif de la défendre, la Cour affirme qu'ils ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée... La principale question qui se pose en l'occurrence sur le terrain de l'article 8 consiste à savoir si les termes du paragraphe 2 suffisent à justifier l'ingérence ainsi constatée. Ménageant une exception à un droit garanti par la Convention, ce paragraphe appelle une interprétation étroite. Caractéristique de l'Etat policier, le pouvoir de surveiller en secret les citoyens n'est tolérable d'après la Convention que dans la mesure stricte-

ment nécessaire à la sauvegarde des institutions démocratiques»[60].

Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel, dans sa recommandation 2/99 concernant le respect de la vie privée dans le contexte de l'interception des télécommunications[61], avait résumé les garanties à respecter découlant de la jurisprudence du Conseil de l'Europe en la matière[62]. Il importe que le droit national, par des dispositions accessibles à tout citoyen[63], précise de façon rigoureuse et dans le respect de toutes les dispositions susmentionnées:

- les autorités habilitées à permettre l'interception légale des télécommunications, les services habilités à procéder aux interceptions et la base légale de leur intervention;
- les finalités selon lesquelles de telles interceptions peuvent avoir lieu, qui permettent d'apprécier leur proportionnalité par rapport aux intérêts nationaux en jeu[64];
- l'interdiction de toute surveillance exploratoire ou générale des télécommunications sur une grande échelle[65];
- les circonstances et les conditions précises (par exemple éléments de fait justifiant la mesure, durée de la mesure) auxquelles sont soumises les interceptions, dans le respect du principe de spécificité auquel est soumise toute ingérence dans la vie privée d'autrui[66];
- le respect de ce principe de spécificité, corollaire de l'interdiction de toute surveillance exploratoire ou générale, implique en ce qui concerne plus précisément les données de trafic que les autorités ne peuvent avoir accès à ces données

60. Sur cet arrêt fondamental et son application en matière d'écoutes téléphoniques par la sûreté de l'Etat, lire B. HAVELANGE et Y. POULLET, «Secret d'Etat et vie privée ou comment concilier l'inconciliable?», colloque international du 20 janvier 1999 organisé par le comité R., *in Droit des technologies de l'information et de la communication, Cahiers du C.R.I.D.*, n° 16, Bruylant, 1999, pp. 235 et s. Sur la notion de démocratie découlant de cet arrêt, l'article de F. OST, «Le concept de 'démocratie', dans la jurisprudence de la Cour européenne des droits de l'homme», *Journ. procès*, 1998, n° 124, pp. 13 et s.
61. Recommandation adoptée le 3 mai 1999 (doc. 5005/99/final, WP 18, déjà cité). Pour rappel, cette recommandation avait été émise dans le cadre des réactions européennes à la découverte du réseau Echelon (cf. *supra*, n° 14).
62. Sur cette jurisprudence, lire le remarquable article de D. YERNAULT, «'Echelon' et l'Europe - La protection de la vie privée face à l'espionnage des télécommunications», *J.T.D.E.*, 2000, pp. 190 et s.
63. A cet égard, la jurisprudence constante du Conseil de l'Europe, D. YERNAULT, «De la fiction à la réalité: le programme d'espionnage électronique global 'Echelon' et la responsabilité internationale des Etats au regard de la Convention européenne des droits de l'Homme», *Rev. belge de droit int.*, 2000, pp. 198 et s. Récemment à propos des écoutes téléphoniques, les condamnations du Royaume-Uni où de simples circulaires du Home Office précisaient les conditions des écoutes, le rapport de la Commission du 14 janvier 1998, *Aff. Govell c. Royaume-Uni*, 6 62 et surtout, l'arrêt de la Cour dans l'affaire *Khan c. Royaume Uni*, 12 mai 2000, ' 27.
64. Sur ces deux premières conditions, on rappellera l'arrêt *Malone* du 2 août 1984: «La loi doit user de termes assez clairs pour indiquer à tous de manière suffisante et sous quelles conditions elle habilite la puissance publique à opérer pareille atteinte secrète» et l'arrêt *Leander* du 26 mars 1987: «Dans un système applicable à tous les citoyens, …, la loi doit user de termes assez clairs pour leur indiquer de manière adéquate en quelles circonstances et sous quelles conditions, elle habilite la puissance publique à se livrer à pareille ingérence secrète, et virtuellement dangereuse, dans leur vie privée … La loi elle même doit définir l'étendue du pouvoir d'appréciation attribué à l'autorité compétente avec assez de netteté - compte tenu du but légitime poursuivi - pour fournir à l'individu une protection adéquate contre l'arbitraire».
65. A cet égard, la déclaration du président de la commission belge de protection de la vie privée, M. Thomas lors de son audition à la commission de la justice de la Chambre lors de l'analyse du projet de loi sur la criminalité informatique (*Doc. parl.*, Chambre, sess. 1999-2000, 50, 0213/004, p. 32): «Il ne faudrait pas en arriver à créer diverses banques de données distinctes et supplémentaires en application du fantasme qui veut que 'cela peut toujours servir'». Cette interdiction d'une surveillance exploratoire et générale est affirmée par l'arrêt *Klass* de la Cour européenne des droits de l'homme déjà cité; elle l'est également par le comité des droits de l'homme de l'O.N.U., observation générale, n° 16.
66. Sur cette condition, les arrêts *Huvig* et *Kruslin* du 24 avril 1990 et l'arrêt *Valenzuela Contreras c. Espagne* du 30 juillet 1998: les garanties à figurer dans la loi concernent «la définition des catégories de personnes susceptibles d'être écoutées, la nature des infractions, la fixation d'une limite à la durée d'exécution; les conditions d'établissement des procès-verbaux de synthèse consignant les conversations interceptées; les précautions à prendre pour communiquer les enregistrements aux fins de contrôle par le juge et la défense; les circonstances dans lesquelles peut et doit s'opérer l'effacement des bandes».

qu'au cas par cas, et non de façon générale et proactive;
- les mesures de sécurité en ce qui concerne le traitement et le stockage des données, et leur durée de conservation;
- en ce qui concerne les personnes impliquées de façon indirecte ou aléatoire dans les écoutes[67], les garanties particulières apportées au traitement de données à caractère personnel: notamment, les critères justifiant la conservation des données, et les conditions de la communication à des tiers[68];
- l'information de la personne surveillée, dès que possible;
- les types de recours que peut exercer la personne surveillée[69];
- les modalités de surveillance de ces services par une autorité de contrôle indépendante[70];
- la publicité - par exemple sous forme de rapports statistiques réguliers[71] - de la politique d'interception des télécommunications effectivement pratiquée;
- les conditions précises auxquelles les données peuvent être communiquées à des tiers dans le cadre d'accords bi ou multilatéraux[72].

22. L'application de ces principes à des mesures qui vont au-delà de la simple interception de communications électroniques pour s'étendre à l'analyse de données de communications antérieures appelle nombre de commentaires. Le prescrit belge réclame de tous les fournisseurs et opérateurs de services de communication électronique le stockage de certaines données de communication sans différencier les personnes concernées. Il est difficile, au vu de tels prescrits, de ne pas parler de surveillance générale. Il y a lieu de craindre, comme le notait le député européen Cappato, rapporteur au Parlement européen dans le débat qui nous occupe, que le surveillé, l'«ennemi», ne devienne «le simple citoyen qui surfe sur le net ou qui passe un coup de téléphone». Cette remarque critique sur la légitimité d'une telle mesure en induit d'autres. Une première consiste à distinguer les traitements, selon leur finalité originaire; la deuxième s'interroge sur la proportionnalité des mesures prises vis-à-vis des risques sensés justifier de telles mesures et la troisième relève les risques créés par les traitements induits par le prescrit en cause.

1. Deux types de traitements

24. Le caractère général du prescrit belge ne distingue pas, à l'inverse de la loi française[73], les données collectées et conservées légitimement par les

67. … Ainsi la personne en lien avec la personne surveillée et sa localisation dans le cas d'un contact par téléphone mobile.
68. Cf. à ce propos, l'arrêt *Amann c. Suisse* (16 février 2000) qui remet en cause les règles de procédure pénale adoptées par la Suisse lorsqu'elles visent «les tiers présumés recevoir ou transmettre des informations à ces dernières (les personnes suspectées ou inculpées)», sans réglementer de façon détaillée le cas de ces interlocuteurs écoutés «par hasard» en qualité de «participants nécessaires» à une conversation téléphonique enregistrée par les autorités … En particulier, la loi ne précise pas les précautions à prendre à leur égard.
69. Sur ces deux dernières conditions, l'arrêt *Buckley* du 25 septembre 1996 ('76) prononcé par la Cour européenne des droits de l'homme, «Selon la jurisprudence constante de la Cour, même si l'article 8 ne contient aucune condition de procédure, il faut que le processus décisionnel débouchant sur des mesures d'ingérence soit équitable et respecte comme il se doit les intérêts de l'individu protégés par l'article 8».
70. Dans l'affaire *Rotaru c. Roumanie* du 4 mai 2000, la Cour exige qu'en dernier ressort même dans le cas d'écoutes administratives, le dernier recours devrait être le pouvoir judiciaire car «il offre les meilleures garanties d'indépendance, d'impartialité et de procédure régulière».
71. Il s'agit d'une exigence rappelée par le groupe dit de Berlin (groupe international de travail sur la protection des données dans le secteur des télécommunications) adoptée lors de la réunion de Hong-Kong le 15 avril 1998, recommandation sur la «Public Accountability in relation to interception of private communications».
72. En particulier dans les réseaux européens de coopération policière et judiciaire comme Europol et Infopol voire, comme souhaité par les Etats-Unis, vers les autorités de défense américaines.
73. Cf. *supra*, n° 18.

opérateurs et fournisseurs de service de communication dans le cadre de leurs propres activités, d'autres données dont la conservation n'est pas *a priori* requise dans le cadre de leurs activités. La directive européenne, nous l'avons vu[74], en dehors du consentement de la personne concernée, légitime la conservation des données pour deux finalités: celle de la facturation et de son paiement et celle de la sécurité du système d'information ou du réseau de cet opérateur et du fournisseur (repérage de tentatives de *hacking*, de sabotage, d'envoi de virus, etc.)[75].

Pour les données conservées et traitées dans le cadre de ces finalités, la communication de telles données aux autorités policières représente un traitement ultérieur au sens des législations de protection des données dont la compatibilité s'apprécie en fonction des principes suivants.

25. En ce qui concerne les données pour lesquelles aucune finalité légitime de conservation n'existe chez l'opérateur ou le fournisseur, la seule finalité légitime réside dans la poursuite d'infractions. En d'autres termes, dans ce second cas, c'est directement l'autorité publique qui est responsable du traitement qu'il confie à l'opérateur ou au fournisseur lui-même voire à un service autre, qui serait chargé de collecter les données provenant des différents opérateurs et fournisseurs. Ces fournisseurs, opérateurs ou services ne sont alors que des sous-traitants et l'article 16 de la directive qui soumet ces sous-traitants et engagement de non-utilisation des données en dehors de la mission confiée) s'applique.

Dans ce second cas, la légitimité de conservation ne peut se fonder que sur les fins d'investigation policière.

Nous sommes des Etats de droit et la Convention à laquelle nous adhérons impose que ceux qui réclament la conservation des données en démontrent l'intérêt social impérieux par rapport aux droits et libertés ainsi diminués. Où sont de telles justifications? Les autorités policières apparaissent bien muettes lorsqu'interrogées à une réunion d'experts convoqués encore ce mois par la Commission européenne pour préparer ce forum, elles s'avéraient incapables de présenter autre chose que des opinions, faits divers là où des études statistiques, sociales et psychologiques auraient pu démontrer qu'effectivement, la préparation active de crimes graves passe par l'utilisation de moyens de communication et qu'effectivement, le travail d'investigation exige l'accès rapide aux données d'une telle utilisation. La confrontation avec les fournisseurs de service a, au contraire, révélé l'imprécision des demandes, leur tâtonnement et la rareté de l'efficacité de telles démarches.

2. Légitimité des traitements d'investigation policière

26. La légitimité des données repose sur un examen de proportionnalité: le risque d'atteinte à la sécurité de l'Etat, à la protection des individus justifie-t-il un traçage «tous azimuts» et le moyen proposé à savoir l'obligation des opérateurs de services de télécommunication, est-il nécessaire à l'obtention de telles fins?

74. Cf. *supra*, n° 19.

75. On rappelle que la première proposition de directive ne mentionnait pas cette finalité, introduite par la suite à la demande des opérateurs. On peut s'inquiéter du caractère vague de cette finalité nouvelle de conservation des données même s'il va de soi que les principes de l'article 6 de la directive dite générale de protection des données s'appliquent et obligent dès lors le fournisseur ou l'opérateur de services de communications à ne procéder à des traitements loyaux que pour des finalités déterminées et compatibles, qu'à propos de données pertinentes et adéquates par rapport à ces finalités et finalement que pour la durée strictement nécessaire.

A cet égard, la gravité du crime est évoquée pour justifier de telles atteintes. On s'interroge. Y a-t-il un lien fort et nécessaire entre le moyen mis à disposition de l'autorité policière et la découverte des délinquants[76]? Non, par contre, on y verra le moyen aisé du traçage d'autres délits bien plus mineurs et directement liés à l'utilisation des technologies de communication, ainsi la violation de droits d'auteur à propos d'oeuvres présentes sur le Net[77], les tentatives de *hacking*, la fraude fiscale, etc. Mais que penser alors d'un discours qui agite le spectre terroriste pour en réalité atteindre une autre cible, celle des délits économiques dont la recherche des auteurs n'apparaît pas justifier le recours aux moyens extraordinaires prévus. Ne faut-il pas en toute hypothèse – et la résolution du Parlement européen déjà évoquée en matière de lutte contre la pornographie enfantine y faisait déjà allusion[78] – réserver à quelques infractions majeures le moyen évoqué?

27. Les règles de proportionnalité, de nécessité, de prévisibilité et de légalité des mesures qui restreignent nos droits et libertés fondamentaux conduisent en toute hypothèse à exiger que la loi précise les limites strictes de la durée de conservation, qu'elle définisse les données d'identification concernées (les seules données de connexion de l'utilisateur et du moment de la «transaction» ne suffisent-elles pas[79]?) et circonscrive à quelques prestataires de services obligés: ceux qui fournissent l'accès aux réseaux, le devoir de conservation. Il faudrait en particulier distinguer les mesures policières ordonnées à propos de données qui sont déjà conservées par les opérateurs de télécoms et celles concernant les autres qui ne seraient conservées qu'à des fins policières.

Il est demandé donc au législateur d'agir ici comme ailleurs avec des «mains tremblantes» d'autant plus que les conséquences du prescrit en question engendrent des risques qu'on énumère ci-après.

3. Les risques de tels traitements

28. Le premier risque est celui de la dérive réglementaire: même avec les limites rappelées ci-dessus et clairement affirmées au départ, on craindra que la loi à peine votée ne voit progressivement son champ élargi et les garanties jugées trop «lourdes» abandonnées dans l'intérêt de l'efficacité. Depuis la première loi belge sur les repérages de communications, cinq autres lois ont suivi élargissant chaque fois un peu les atteintes des autorités policières aux

76. Poussons le raisonnement à l'absurde. Tirera-t-on du fait qu'il semble que les complices de Ben Laden - pour autant que celui-ci soit coupable - disposaient pour opérer l'attentat de lames de rasoir, la conséquence de la nécessité du fichage de tout individu achetant de telles lames?

77. A noter à cet égard, la résolution adoptée par le Parlement européen du 4 mai 2000 et la communication de la Commission européenne du 30 novembre 2000 à propos de la lutte contre la contrefaçon et le piratage dans le marché unique qui encourage précisément la collaboration du secteur privé et des autorités policières et judiciaires dans leur lutte pour la protection de la propriété intellectuelle. Une proposition de directive est attendue sur ce point pour octobre de cette année.

78. Cf. *supra*, n° 14 *in fine*.

79. Il s'agit «d'exclure, dans la rédaction du décret, les données de communication pouvant être considérées comme des données indirectes de contenu ou de comportement. Certaines données techniques peuvent en effet fournir des éléments sur le contenu des informations transmises (par exemple, l'URL des sites visités, l'adresse IP du serveur consulté ou l'intitulé d'un courrier électronique), ou sur le comportement des internautes (adresse du destinataire d'un courrier électronique par exemple). Le forum considère que ce type de données ne doit pas être mentionné dans le décret en préparation. En revanche, il considère que l'adresse IP de l'utilisateur relève bien des données nécessaires à l'établissement de la communication et n'indique rien quant au contenu des informations consultées ou au comportement de l'internaute». (forum des droits sur l'Internet, recommandations aux pouvoirs publics: conservation des données relatives à une communication électronique, 18 déc. 2001, disponible à http://www.foruminternet.org/recommandations/lire.phtml?id=230).

secrets des communications. Ainsi, dira-t-on demain, puisque de tels réservoirs de données existent, ne peut-on y recourir plus largement[80]? Cette tendance, une fois introduite une exception, à y en ajouter d'autres inquiète. Comment sur ce point, ne pas louer la sagesse américaine du «Patriot Act» qui limite à l'horizon de quatre ans, les mesures exceptionnelles attentatoires aux libertés, qui y sont contenues et d'ajouter que parmi ces mesures, celle d'obliger à la conservation des données n'y est même pas reprise.

Parmi les premières réactions négatives à ces mesures, les avocats ont souligné le danger que représentaient pour eux les atteintes ainsi facilitées au secret professionnel. L'autorité policière aura en effet quelques difficultés à démêler *a priori* parmi toutes les communications dont elle ordonnera le relevé, celles couvertes par le secret professionnel et les autres.

Ensuite, on rappellera que le renforcement de la cybersurveillance exige son contrôle par une autorité indépendante. Est-on sûr que le contrôle des investigations menées sur le terrain par des équipes policières bien entraînées sera effectif, que les autorités judiciaires ou spécifiques de contrôle pourront toujours saisir la portée des utilisations faites des moyens nouveaux d'investigation. En outre, la circulation d'informations au sein des réseaux de collaboration internationaux ou européen n'exige-t-elle pas un renforcement des contrôles démocratiques ou juridictionnels d'Europol, d'Interpol, du futur «Eurojust» ou d'Enfopol[81]?

29. D'autres risques de dérive étaient déjà soulignés par la commission belge de protection de la vie privée[82] lors du débat ayant mené au vote de la loi sur la criminalité informatique. La simple existence de tels fichiers crée en toute hypothèse des risques de dérive: les prestataires contraints à un tel stockage peuvent être tentés de rentabiliser leurs prestations à d'autres fins. Au-delà de la sécurisation de leurs propres services ou réseaux, on songe au profilage des utilisateurs à des fins propres ou de commercialisation. Certes on pourrait songer confier la gestion de tels fichiers à des tiers spécialisés en conservation, *a fortiori* aux autorités policières mais c'est substituer au risque décrit, celui plus grand encore de fichiers mammouths où toutes les interconnexions deviennent possibles.

30. Si la Cour européenne des droits de l'homme considère que le seul stockage de données à des fins policières est déjà une atteinte à nos libertés (Affaires *Klaas, Lüdi, Rotaru, Ammann*,...), les conséquences des traitements induits par les législations évoquées ci-dessus appellent des pré-

80. Ainsi, le débat en cours en France à propos de l'intérêt porté par l'administration fiscale aux données de connexion. Le Sénat a adopté le 18 décembre, dans le cadre du projet de loi de finance rectificative 2001, des amendements donnant accès pour les agents des douanes et les enquêteurs de la commission des opérations de bourse (C.O.B.) aux données conservées par les fournisseurs d'accès et les opérateurs télécommunications au titre de la L.S.Q. Il en profite cependant pour proposer un nouvel amendement qui étend ce droit d'accès aux agents de l'administration fiscale. Par le biais d'un nouvel amendement, modifiant l'article L 32-3-1 du Code des postes et télécommunications, il complète également le dispositif en prévoyant que «Pour les besoins de la recherche, de la constatation de la sanction ou du règlement d'infractions aux dispositions du Code des douanes, du Code général des impôts ou du Code monétaire et financier, les opérateurs (...) et les prestataires mentionnés aux articles 43-7 et 43-8 de la loi du 30 septembre 1986 (...) doivent communiquer (...) les données qui leur sont demandées par les agents habilités à cet effet, de l'administration des douanes et des services chargés du recouvrement des impôts, droits et taxes (...)». Les agents de l'administration fiscale obtiennent donc un droit d'accès aux données conservées par les opérateurs au titre de leur facturation.

81. A cet égard, lire H. BRULIN et D. MOREAU, «Coopération policière internationale et autorités de contrôle... Mariage d'amour ou de raison?», *in Droit des technologies de l'information - Regards prospectifs*, E. MONTERO (ed.), Bruylant, Bruxelles, 1999, pp. 185 et s.

82. Avis de la commission belge de protection de la vie privée, déjà cité *supra*, note 5.

cautions bien plus importantes encore. En effet, on peut craindre que les forces de police ne puisent dans ces vastes réservoirs de données les premiers éléments de leur enquête et ce, avant même toute autre investigation (repérage des personnes à proximité du lieu de commission de l'infraction, liste des correspondants, dernier appel entrant ou sortant...). Pire, elles peuvent être tentées d'y trouver les moyens d'une surveillance exploratoire de groupes dits «à risque», ceux qui furètent tel ou tel site, ceux qui se connectent au réseau à partir de tel ou tel endroit, jugé chaud, les présumés «terroristes» ou *hackers*, etc.

Ainsi, il est absolument requis «d'interdire toute mise en place par les services de sécurité d'un accès général aux informations sauvegardées: l'interrogation des données conservées doit se faire dans le cadre d'une procédure précise, sur une base de requêtes au cas par cas. Il ne saurait être possible d'instaurer un accès permanent à ces données permettant la mise en place de traitements automatisés pouvant s'apparenter à une surveillance générale des réseaux. La conservation physique de ces données devra donc relever de la seule responsabilité des entreprises visées qui devront en limiter strictement l'accès»[83].

4 Conclusions[84]

31. La lutte contre la cybercriminalité est affirmée comme une priorité sans laquelle nos sociétés ne pourraient survivre. Au nom de la sécurité, forts de l'opinion publique relayée et amplifiée par les médias, les pouvoirs politiques préparent dans la hâte, tant au niveau national qu'européen des législations accroissant les pouvoirs des autorités judiciaires et policières afin de mener une lutte efficace contre la cybercriminalité et le terrorisme. Osera-t-on leur rappeler que les bandes de Ben Laden, à supposer qu'elles soient coupables des événements du 11 septembre, ne semblent point avoir eu besoin des vertus d'Internet pour commettre leur crime et qu'Echelon n'a pas permis de déjouer leurs plans?

Que disent ces législations écrites à la diable? Elles obligent les divers fournisseurs de services de communications électroniques privées ou publiques - et ils sont nombreux - de conserver pendant un délai que d'aucuns estiment d'un an (notre législation belge fixe ce délai comme minimal!)[85] les données qui résultent de notre utilisation de ces services et ce indépendamment d'une utilisation pour la fourniture de service de télécommunication. On crée des données sur toute la population pour les fins préventives de lutte contre la criminalité et ce sans soupçon concret.

Sans doute, objectera-t-on aux défenseurs des libertés, que la liberté

83. Forum des droits sur l'Internet, recommandations aux pouvoirs publics: conservation des données relatives à une communication électronique, 18.12.2001, disponible à http://www.foruminternet.org/recommandations/lire.phtml?id=230. Sans doute, est-il à recommander également que la conservation tant par les fournisseurs et opérateurs que par les autorités policières s'opère avec des «logiciels libres» permettant d'éviter que des manipulations puissent avoir lieu de manière non détectable par les autorités de contrôle.
84. Nos conclusions reprennent certains passages de l'exposé de l'auteur lors de l'audition organisée par la Commission européenne à Bruxelles le 27 novembre, audition relative à la lutte contre la cybercriminalité. L'intervention a été publiée *in extenso* sous le titre «Sécurité ou Libertés?», *Ubiquité, Revue de droit des technologies de l'information*, Larcier, Bruxelles, 2002, pp. 3 et s.
85. Cf. sur ce point, *supra*, n° 4.

prônée est un luxe, alors même que certaines vies sont en danger. On ajoutera que l'homme honnête n'a rien à craindre de cette surveillance mieux assurée qui débusque les méchants et n'effraie pas le gentil. Certains iront jusqu'à évoquer le mérite de cette surveillance qui force à adopter un comportement toujours plus conforme aux normes sociales.

28. A ceux là qu'il me soit permis de répondre. Il n'est selon moi pire danger que cette cybersurveillance qui traque l'homme dans son intimité et crée chez lui la hantise perpétuelle du dévoilement. «Par un renversement pervers, cette prééminence obsessionnelle du regard de l'autorité[86] se fait au nom même de ce qu'elle détruit. Les valeurs derrière lesquelles elle s'abrite sont de haut vol: justice, liberté, démocratie, respect des lois, civisme, intégrité. Mais qui ne voit que derrière cette vision, décapante parfois à force d'user les cibles sur lesquelles elle porte, lime jusqu'à l'os certains principes qui fondent le vouloir vivre ensemble? Quand la proportionnalité n'est plus respectée entre les moyens que se donne l'investigation et les buts recherchés, la sacralisation de l'investigation et du dévoilement assoit comme légitimité unique le moyen et non plus la cause [87]».

En plus de telles mesures qui créent artificiellement un sentiment de sécurité évitent que ceux qui les prennent s'interrogent sur le pourquoi du crime et les instruments de politique criminelle qui permettent de faire face à cette montée de violence. Tout passe par la criminalisation et la défense de la société sans interrogation supplémentaire. Or on le sait, la criminalité finit toujours par se déplacer ou devenir plus violente si on ne s'attaque pas réellement à ses causes.

86. A cet égard, les réflexions de J. BOYLE «Foucault in Cyberspace: Surveillance Sovereignty and Hard-Wired Censors, disponible à http://www.wel.american.edu/pub/faculty/boyle/fouc1.html.». L'auteur compare les systèmes policiers de surveillance électronique à un «panopticon» virtuel bien plus efficace que celui réel proposé par J. BENTHAM.
87. B. FRAPPAT, «La dictature de la transparence», *Etudes*, 1999, p. 58.